



Department of Homeland Security Daily Open Source Infrastructure Report for 21 October 2005

Current
Nationwide
Threat Level is
ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS
[For info click here](http://www.dhs.gov/)
<http://www.dhs.gov/>

Daily Highlights

- The Associated Press reports Vermont Technical College mistakenly posted every student's Social Security number on the Internet for almost two years, when the data was inadvertently sent to the public Website instead of a secure computer drive. (See item [6](#))
- The Federal Railroad Administration has given the nation's railroads 30 days to fix a growing safety problem with an increasing number of train crashes due to track switches left in the wrong position. (See item [13](#))
- The Washington Post reports Virginia's George Mason University's Center for Health Policy, Research and Ethics has been tasked to develop a state plan for evacuation response. (See item [24](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *October 20, Associated Press* — **Six percent of customers still without power in Louisiana.** According to the Louisiana Public Service Commission, six percent of customers (130,000 customers) remain without power because of Hurricanes Katrina or Rita. Five percent of customers (269,000) are without phone service. Most of the disadvantaged are located in

Orleans and St. Bernard parishes.

Source: <http://www.katc.com/Global/story.asp?S=4003979&nav=EyB0>

2. *October 19, Journal News (NY)* — **Tritium found in wells at Indian Point.** The Nuclear Regulatory Commission (NRC) has confirmed that tritium, a hydrogen isotope, has been leaking from a spent–fuel storage tank at Indian Point nuclear power plant since late August. NRC sampled five underground wells and found trace elements of the isotope, which gives off a weak radiation. Representatives for Entergy Nuclear Northeast, which owns the two reactors, said that the levels of tritium found are well below the amount allowed by the Environmental Protection Agency for drinking water and do not pose a threat to the public or to workers. NRC officials participated in a multi–agency conference call on Tuesday, October 18, at which Entergy shared plans to determine the cause of the leak and its effect on the surrounding area. The facility is located in Buchanan, NY.

Source: <http://www.thejournalnews.com/apps/pbcs.dll/article?AID=/20051019/NEWS02/510190373/1018>

3. *October 19, Utility Automation and Engineering Magazine* — **Advanced distributed energies could be used to protect power supplies to critical infrastructure during disasters.** According to the Department of Energy’s Federal Energy Management Program, local energy is important to the development of security solutions at federal facilities, a concept which could apply to the re–development and re–fitting of cities to prepare for disasters. John Kelly, executive director of distributed energy technology research at The Gas Technology Institute (GTI), supports this effort. He says: "Hurricane Katrina proved just how dark it can get when critical, life–sustaining services are incapacitated because of reliance on an antiquated, fragile, centralized utility grid... If more of the electricity in the nation were dispersed locally, at the point of use, the adverse consequences of threats to power infrastructure would be diminished." GTI supports the development of a hybrid electric system design that “leverages a number of advanced, small–scale power generation technologies” that would help protect critical facilities and functions, according to Kelly. Cities including Philadelphia, San Diego, and Chicago, currently use distributed energy technologies to produce power, and commercial real estate owners in New York have developed distributed energy master plans.

Source: http://uaelp.pennnet.com/Articles/Article_Display.cfm?ARTICLE_ID=239419&p=22

4. *October 18, Denver Post* — **Pilot program uses wind to create battery of stored power.** Xcel Energy and the National Renewable Energy Laboratory (NREL) plan to use power generated by wind farms during off–peak hours to produce hydrogen that would in turn be used later, during periods of peak demand, to produce additional electricity. The hydrogen essentially becomes a battery to store wind power. The technology is one of the first attempts to combine the two energy resources. Frank Novachek, director of corporate planning for Xcel Energy, says, "This helps us get more value out of wind energy and helps advance the prospects of hydrogen." The hydrogen produced would generate enough electricity to power 20 to 25 homes.

Source: http://www.denverpost.com/search/ci_3126273

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

5. *October 19, NBC 5 (IL)* — **Chemical plant blaze prompts road closure, worries residents in Chicago.** Investigators say chemicals fueled the flames of a massive factory blaze near the Southwest Side of Chicago, IL, that began late Tuesday night, October 18. The fire broke out around 11 p.m. CDT at a chemical factory at 15th and Ashland, resulting in nearby street closures. Firefighters were still on the scene at 5:30 a.m. CDT, when some chemicals started to flare up. At its height, the blaze required more than 200 firefighters as flames shot 20 to 30 feet above the roof of the structure. The fire knocked out power to the area and temporarily shut down a nearby Metra line, which was running normally by 6 a.m. Crews were able to prevent the fire from spreading to nearby buildings. Ashland was closed between Roosevelt and 16th streets, and officials did not say when it would reopen. The No. 9 Ashland bus was temporarily rerouted around the closure, but was back on a regular schedule late Wednesday morning, October 19. Cortez Trotter, the Chicago Fire Department commissioner, said 55-gallon drums inside the factory were the likely source of the explosions.
Source: <http://www.nbc5.com/news/5122580/detail.html>

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report.

[\[Return to top\]](#)

Banking and Finance Sector

6. *October 20, Associated Press* — **Vermont college mistakenly posts students' personal information.** Vermont Technical College, located in Randolph Center, VT, mistakenly posted every student's Social Security number on the Internet for almost two years, college officials said. The data, along with names, addresses, SAT scores and ethnicities, were removed last week, and there was no indication that the information was downloaded by identity thieves, officials said. The 2003 information was publicly posted in January 2004 when the college's coordinator of tutoring services tried to direct it to a secure computer drive but inadvertently sent it to the public Website instead, college President Allan Rodgers said. The error was discovered last week by a former student who plugged his own name into the Google search engine.
Source: <http://abcnews.go.com/US/wireStory?id=1233752>
7. *October 20, New Zealand Press Association* — **New Zealand customs seize large amount of counterfeit United States currency.** A man traveling from Sydney, Australia, has been caught at a New Zealand airport with almost \$US1.3 million in counterfeit notes. Mustafa Yousif Ibrahim was arrested at Auckland International Airport as he came off a flight from Sydney on Wednesday, October 19. Ibrahim was born in Sudan but is believed to have been made a New Zealand resident in the early 1990s after arriving as a refugee. According to a police summary of the facts, 158 separate bundles of American currency were found. Each of the bundles comprised 80 \$US100 notes, with the total amount found coming to \$US1.26 million, police said. Police said Ibrahim could not give "any logical explanation" for having the money. He

appeared in court on one charge of being in possession of forged currency. Ibrahim, who said he was unemployed, was remanded on bail for two weeks and has had to hand over his passport to the police.

Source: <http://www.smh.com.au/news/world/nz-customs-seize-huge-stash-of-counterfeit-cash/2005/10/20/1129775897065.html>

8. *October 20, NZ City (New Zealand)* — **Bank takes Internet banking facility offline due to scam.** The Bank of New Zealand's Internet banking Website was offline on Thursday, October 20, after reports of customers being targeted by a phishing scam. The bank said it became aware of the latest scam targeting its online customers at about 1 p.m. local time Thursday, and took its banking Website offline at that time. The Website may be online again by Friday, October 21, but is likely to be without some of its functions until further notice.

Source: <http://home.nzcity.co.nz/news/default.asp?id=56016&c=w>

[[Return to top](#)]

Transportation and Border Security Sector

9. *October 20, Associated Press* — **Los Angeles Airport controller was tired when near crash occurred, report says.** A report released this week by the National Transportation Safety Board (NTSB) noted a controller was tired when a near crash at Los Angeles International Airport occurred, and the control tower was staffed at about half its normal level at the time of the August 2004 event. But it does not offer an official cause of the near disaster, which occurred on a clear afternoon. The incident unfolded when the controller positioned a departing Southwest jet on the same runway on which an Asiana jumbo jet was cleared to land. The Asiana pilot saw the Southwest jet and pulled up as alarms sounded in the control tower. The planes missed each other by 200 feet. The controller handling the planes had just relieved another controller who needed a break. The departing controller told his replacement that he had cleared the Asiana jet to land, according to the report. According to the NTSB report, the controller handling the jets told investigators he had worked the previous evening and had slept no more than six hours before returning to the tower for a morning shift. The NTSB is continuing to investigate the incident.

Source: http://www.usatoday.com/travel/news/2005-10-20-lax-controller_x.htm

10. *October 20, South Florida Sun-Sentinel* — **Hurricane forces Amtrak cancellations.** With Hurricane Wilma looming, Amtrak has canceled train service between Orlando and Miami through the weekend, and has canceled the Auto Train runs Friday, October 21, between Florida and Virginia. Amtrak announced the service is being canceled because of safety precautions and said additional service changes could be forthcoming as the hurricane's path becomes clearer. The Silver Star and Silver Meteor trains which normally run between New York and Miami will continue between New York and Orlando but will not run to and from Miami through the weekend.

Source: <http://www.sun-sentinel.com/news/local/southflorida/orl-bk-amtrak102005.0,494611.story?coll=sfla-home-headlines>

11. *October 20, Union Tribune (CA)* — **'Grenade' in Ontario terminal was a gear shift knob.** A

terminal at California's Ontario International Airport was evacuated Thursday morning, October 19, after airport security detected what appeared to be a hand grenade in a piece of luggage. The object turned out to be an automobile gear shift knob that had been made to look like a grenade, said airport spokesperson Maria Tesoro-Fermin. Baggage screeners with the Transportation Security Administration spotted the suspicious-looking object about 6 a.m. PDT. The upper level of the airport's Terminal 2 was immediately cleared and Ontario police, firefighters, and bomb disposal technicians were called to the scene. A bomb squad blew up the bag about 8:30 a.m. and passengers were allowed to re-enter the terminal about an hour later, Tesoro-Fermin said. The airport is about 35 miles east of Los Angeles.

Source: http://www.signonsandiego.com/news/state/20051020-0957-bn20g_renade2.html

12. *October 20, Government Accountability Office* — **GAO-06-181T: Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts**

(Testimony). The July 2005 bombing attacks on London's subway system dramatically highlighted the vulnerability of passenger rail systems worldwide to terrorist attacks, and the need for an increased focus on security for these systems. This testimony provides information on how the Department of Homeland Security (DHS), including the Transportation Security Administration (TSA) and the Office for Domestic Preparedness have assessed risks posed by terrorism to the U.S. passenger rail system using risk management principles; actions federal agencies have taken to enhance the security of U.S. rail systems; and rail security practices implemented by domestic and selected foreign passenger rail operators and differences among these practices. The Government Accountability Office's (GAO) September 2005 report on passenger rail security recommended, among other things, that TSA develop a timeline for completing its methodology for conducting risk assessments, and develop rail security standards that reflect industry best practices and can be measured and enforced. GAO also recommended that the Secretary of DHS determine the feasibility of implementing certain security practices used by foreign rail operators. DHS, the Department of Transportation, and Amtrak generally agreed with the report's recommendations.

Highlights: <http://www.gao.gov/highlights/d06181thigh.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-181T>

- 13. *October 19, Department of Transportation* — **Railroads have 30 days to fix problem of misaligned track switches.**** The nation's railroads have been given 30 days to fix a growing safety problem with an increasing number of train crashes due to track switches left in the wrong position, Department of Transportation Secretary Norman Y. Mineta announced on Wednesday, October 19. Mineta said his department's Federal Railroad Administration has set a November 22 deadline in an emergency order mandating all railroads take specific and immediate steps to end the problem, which has led to nine serious train crashes, ten fatalities, and injuries to more than 600 people since January. The accidents have occurred when employees working in areas not equipped with remote electronic signal monitors failed to follow track-switching procedures, Mineta said. In every case, the failure to reset the hand-operated switches has led to trains running onto the wrong tracks and derauling or colliding with locomotives or rail cars or both, he added. The emergency order mandates that railroads retrain and periodically test employees on switch operating procedures and increase communication among crewmembers regarding the position of the switch. Specifically, employees must be briefed on the use of switches and provide written documentation every time a switch is moved. In addition, locomotive engineers must acknowledge that switches are

properly set before trains can be operated.

Source: <http://www.dot.gov/affairs/fra2705.htm>

[\[Return to top\]](#)

Postal and Shipping Sector

14. *October 20, DM News* — Higher fuel costs worry USPS, but it's ready for busy fall. The U.S. Postal Service (USPS) is preparing to handle an expected increase in volume this fall — most of it Standard mail — over last year, but postal officials expressed concern last week about the need to keep fuel costs down. The USPS' biggest concern this year is keeping fuel costs down. "Fuel is having a tremendous detrimental effect on the cost of the logistics network," said Tony Pajunas, USPS manager of logistics. "Every penny increase in the price of fuel costs is worth \$8 million more a year to us. When you think about all the pennies that fuel has gone up over the past few months, it is adding in excess of \$100 million to the bottom line." Despite fuel costs, the USPS again will extend its surface reach. Though the USPS may normally truck First-Class mail 700 miles, it might stretch it to 1,000 miles "to make room on the planes for the packages that have to fly to get timely service."

Source: http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=3442_8

[\[Return to top\]](#)

Agriculture Sector

15. *October 20, Agricultural Research Service* — Scientists seeking biocontrols against sharpshooters. A parasitic wasp could help California grape growers ward off the glassy winged sharpshooters (GWSS) that have been spreading plant-damaging *Xylella fastidiosa* bacteria in southern California vineyards since the 1990s. Now sharpshooters have made it to Hawaii, and Tahiti. ARS scientists have shown that the invasive GWSS in California is from Texas — part of the pest's native habitat. *X. fastidiosa* causes a variety of costly plant diseases, including Pierce's disease in grapevines and leaf scorch in oleanders. Grape growers in Riverside and San Diego counties have lost about \$38 million due to Pierce's disease. At the ARS South American Biological Control Laboratory (SABCL) in Argentina, researchers have been evaluating wasps that lay their eggs inside GWSS eggs, which are later consumed by the wasp young as they hatch and feed. The primary candidate for this form of biological control is currently *Gonatocerus tuberculifemur* from South America. *G. tuberculifemur* is being tested at both the SABCL and the Beneficial Insects Research Unit in Texas, but the wasp has not yet been released. Researchers in Texas are also searching for nymphal parasitoids in their native range in Texas. To date, all the biological control *Gonatocerus* species agents are egg parasitoids.

GWSS information: <http://info.ucr.edu/gwss/>

Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

16. *October 19, Indiana Ag Connection* — Ash borer found south of Fort Wayne. A tree-killing beetle has been spotted south of Fort Wayne, IN. And the Indiana Department of Natural Resources has quarantined ash products from two townships in Adams County. The state

applied the quarantine to Root and Washington townships after the Decatur city forester reported finding emerald ash borer larvae and an adult on an ash tree in the city about ten miles west of the Ohio State line and 20 miles south of Fort Wayne. A Purdue University specialist says the beetle may have been at the site as long as five years, long before it was first confirmed in Indiana. The beetle has been found in Michigan, northern Ohio, Indiana, and southern Ontario, Canada.

Multistate emerald ash borer Website: <http://www.emeraldashborer.info/>

Source: <http://www.indianaagconnection.com/story-state.cfm?Id=636&yr=2005>

17. *October 18, Associated Press* — Rita losses for farmers estimated at \$195 million or more.

Hurricane Rita cost farmers at least \$195 million in crop and livestock losses, pushing the total for that storm and Hurricane Katrina past \$1 billion, the U.S. Department of Agriculture (USDA) said Tuesday, October 18. The USDA released a preliminary assessment of agricultural damage from Rita, which inundated the Gulf Coast with high winds and heavy rains after making landfall September 24. Analysts cautioned that damage information is changing daily and that estimates don't include long-term losses, such as those from buildings, fences, and machinery. Estimates of losses from Hurricane Katrina, released last month, placed damage at \$882 million. Farm-raised fish, shrimp, and shellfish took the biggest hit from Rita, with losses estimated at \$80 million. The fish and shellfish industry in Louisiana, Mississippi, and Texas generated cash receipts of \$334 million last year. Rita hit virtually all the sugarcane fields in Louisiana, where growers sustained \$42 million in losses to processed sugar. Rice growers had already harvested much of their crop in Louisiana and Texas, but enough was not yet harvested for Rita to cause losses of \$24 million. Soybean losses were estimated at eight million dollars, sorghum losses at seven million dollars, and corn losses at two million dollars.

Source: <http://www.signonsandiego.com/news/business/20051018-1424-farmlosses.html>

[\[Return to top\]](#)

Food Sector

18. *October 19, Associated Press* — Agriculture commissioner confiscates Vietnamese basa

fish. The Georgia Department of Agriculture seized 915 pounds of Vietnamese basa fish Wednesday, October 19, because samples tested positive for a banned antibiotic, state officials said. Agriculture Commissioner Tommy Irvin said that Georgia's food safety lab confirmed the presence of enrofloxacin and the fish have been placed under a "Stop Sale" order until officials can oversee the destruction of the fish. The antibiotic was found in frozen fish labeled "Blue Ocean Basa Fillets Frozen" sold at a retail store in Norcross, GA, and in fish labeled "IQF Basa Fillets" sold at a Suwanee, GA, wholesale business. State officials are working with distributors to find other places where the fish were shipped. On October 4, Alabama officials said more than 204,000 pounds of Vietnamese fish in Alabama warehouses will have to be destroyed because testing found mislabeling and widespread use of an illegal antibiotic.

Source: <http://www.macon.com/mld/macon/news/politics/12944094.htm>

[\[Return to top\]](#)

Water Sector

19. *October 19, Associated Press* — **Officials to see if tainted water reaching Hudson River or drinking water supply.** Experts will study the contours of the earth and rock beneath the Indian Point nuclear power plants to see if the slightly radioactive water that has been found underground could end up in the public drinking supply or the Hudson River. The Nuclear Regulatory Commission (NRC) and Entergy Nuclear Northeast, which owns the plants in Buchanan, NY, said Wednesday, October 19, that low levels of tritium — a radioactive isotope — have been found in water at the bottom of six sampling wells on the Indian Point property. In one of the wells, the amount of tritium is slightly above the federal standard permitted for drinking water, said NRC spokesperson Neil Sheehan. However, none of the wells, which are 20–30 feet deep, are used for drinking water or for anything other than sampling groundwater, said Jim Steets, Entergy spokesperson. Steets said previous studies have shown that water moves parallel to the Hudson and not into it, "but since then we've put buildings on the site so we have to look to see how that may have impacted the hydrology." The new study will help Entergy determine where to dig more wells to test the water, he said.
Source: <http://www.newsday.com/news/local/wire/newyork/ny-bc-ny--indianpoint1019oct19.0.83071.story?coll=ny-region-apnewyork>

20. *October 19, U.S. Environmental Protection Agency* — **Drinking water agreements made with 24 domestic airlines.** The U.S. Environmental Protection Agency (EPA) has reached settlements with 11 major domestic airlines and 13 smaller airlines to ensure the safety of the drinking water used by their passengers and crew. The settling airlines have agreed to routinely monitor the quality of water on their airplanes. The action came after an EPA investigation of 327 U.S. and foreign planes at 19 airports in 2004 found total coliform contamination in the drinking water in 15 percent of aircraft. Total coliform is an indicator that other disease-causing organisms could be in the water and could potentially affect people's health. The settlements require the airlines to regularly monitor aircraft water systems; notify EPA and the public when tests reveal contamination; and regularly disinfect aircraft water systems and water transfer equipment. The orders also require each airline to study possible sources of contamination from outside of the aircraft.
Airline water supply regulation information: <http://www.epa.gov/airlinewater>
Source: <http://yosemite.epa.gov/opa/admpress.nsf/d9bf8d9315e942578525701c005e573c/0b6df456b61c61fa8525709f0064c1c7!OpenDocument>

[\[Return to top\]](#)

Public Health Sector

21. *October 20, Associated Press* — **Thirteenth person dies of bird flu in Thailand.** A 48-year-old man died of bird flu in Thailand after handling his neighbor's sick chickens. Thai Prime Minister Thaksin Shinawatra said Thursday, October 20, new lab results confirmed the country's 13th death from the H5N1 strain of bird flu. Initially, authorities said the man had tested negative for the virus. The dead man, Bang-on Benphat, was hospitalized with pneumonia-like symptoms on Sunday, October 16, shortly after he cooked and ate his neighbor's dead chickens. His seven-year-old son, who also had contact with the chickens, has been hospitalized in Bangkok with a fever and lung infection and is also suspected of having bird flu, said Thawat Suntrajarn, director-general of the Department of Communicable Disease

Control. Taiwan, also, confirmed on Thursday, October 20, the island nation's first case of the disease in birds smuggled in from China. More than 60 people have died of bird flu since late 2003, all of them in Asia. Most human cases have been linked to contact with sick birds. But health officials warn the virus could mutate into a form that can be easily passed between humans, possibly triggering a global pandemic which could kill millions.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2005/10/20/AR2005102000328.html>

22. *October 19, Government Executive* — House panel to probe federal medical response capacity. A congressional panel is trying to understand how the federal government provides doctors, medicine, and supplies to affected areas following a disaster. The House Homeland Security Committee is slated to hold a hearing Thursday, October 20, focusing on how the federal medical response to hurricanes Katrina and Rita reflect the government's readiness to respond to biological or nuclear terrorist attacks.

Source: [http://www.govexec.com/story_page.cfm?articleid=32597&dcn=to daysnews](http://www.govexec.com/story_page.cfm?articleid=32597&dcn=to%20daysnews)

23. *October 19, Associated Press* — Fifth Amish child in Minnesota has polio. State health officials have confirmed a fifth case of poliovirus infection in an Amish child in central Minnesota, the Minnesota Health Department said Wednesday, October 19. The child's family is unrelated to two other families with children who have also tested positive for the virus, said Doug Schultz, a Health Department spokesperson. The families are all part of the same Amish community near Clarissa. The latest infected child doesn't have any symptoms of paralytic polio, Schultz said. State epidemiologist Harry Hull last week said he expects more cases of polio infection to turn up as community members are tested. Health officials have been canvassing the community, many of whose members are unvaccinated, urging them to be tested and immunized. The first case appeared in an infant hospitalized for health problems related to a compromised immune system. The virus then spread to three siblings of a family that wasn't related to the infant's family but had direct ties.

Source: <http://www.twincities.com/mld/twincities/news/12943987.htm>

[\[Return to top\]](#)

Government Sector

Nothing to report.

[\[Return to top\]](#)

Emergency Services Sector

24. *October 20, Washington Post* — Virginia to develop plans for evacuation response.

Hurricane Katrina hit and Virginia wanted to help. An emergency shelter was set up to handle 1,000 evacuees at Fort Pickett, an Army National Guard base southwest of Richmond, VA. Although Gulf evacuees were sent to various sites, "Town Picket," as it was quickly dubbed, never received a single evacuee. Still, Virginia officials said they learned much from the experience. So Governor Mark R. Warner has assigned George Mason University's Center for Health Policy, Research and Ethics in Fairfax, VA, to develop a state plan for evacuation

response. He also ordered a report on the lessons learned from launching Town Pickett and getting it ready for victims of Hurricane Katrina. "This was the first time the nation had to displace so many people," said Peggy Jo Maddox, deputy director of the George Mason health policy center. "All the states had to scramble. So we're going to document what it takes to start up an evacuation center, because no one has ever had to do this before." The George Mason center plans to have the report ready by December, Maddox said.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2005/10/19/AR2005101900053.html>

25. *October 20, Washington Post* — **Maryland county examines crisis responses.** A staged emergency exercise Tuesday, October 18, was a test of how Howard County, MD, police and fire officials would react if a stolen, leaking barrel of poison were discovered. It was part of the county's first Community Readiness Week, during which officials conducted emergency scenarios and tested new communications equipment. Thursday, October 20, officials with the Community Emergency Response Network and Howard County General Hospital announced the creation of a medical reserve corps unit, a group of 18 medical professionals who would work with first responders and could establish a mobile hospital if Howard County General Hospital were filled in a disaster. Also this week, the county will test its new automated telephone dialing system, which sends a recorded message to homes and offices during a disaster.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2005/10/19/AR2005101901045.html>

26. *October 20, East Bay RI* — **Rhode Island high school — site for a mock disaster to test interagency coordination.** Tuesday, October 18, Barrington High School in Barrington, RI, was the site picked to host a full-scale mock disaster, which featured emergency personnel from Barrington, Bristol, Warren, East Providence, Providence and the Rhode Island state police. The Rhode Island Emergency Management Agency organized the event in order to better prepare municipal and state agencies in the case of a real disaster. The mock disaster plan called for the release of a "dangerous" chemical agent. Within a half hour from the start of the scenario, an East Providence Fire Department vehicle pulling a decontamination trailer arrived at the school. Firemen on site quickly converged on the vehicle, pulled on suits and set up two bright yellow decontamination tents. Other events occurred in quick succession — another fire engine arrived, without sirens, followed by an ambulance, and then the S.W.A.T. team. The entire event was paid for with state funding and was under the direction of the Rhode Island Emergency Management Agency. Nathan Rogers, Homeland Security Exercise and Evaluation Director, oversaw the exercise.

Source: <http://www.eastbayri.com/story/284507782278412.php>

[\[Return to top\]](#)

Information Technology and Telecommunications Sector

27. *October 19, Los Angeles Times* — **Glitch results in phone outages for thousands.** At least 150,000 customers in Southern California lost their phone and Internet service for up to 12 hours Tuesday, October 18, because of a computer glitch at a Long Beach central switching plant. The outage struck communities from Hermosa Beach to Newport Beach along the coast

and as far inland as Whittier and Garden Grove. According to Verizon, the problem was caused by a software error in a downtown Long Beach office of Verizon Communications Inc. The malfunction corrupted the main software that connects calls and operates the local network. Source: <http://www.latimes.com/news/printedition/la-me-phones19oct19.1.4316471.story?ctrack=1&cset=true>

28. *October 19, FrSIRT* — Netscape browser security update fixes multiple vulnerabilities. Multiple vulnerabilities have been identified in Netscape. These could be exploited by malicious Websites to execute arbitrary commands or conduct spoofing attacks. The severity of this vulnerability depends on the value of servers which might be vulnerable to HTTP request smuggling and similar attacks, or which share an IP address (virtual hosting) with the attacker's page. For users connecting to the Web through a proxy this flaw could be used to bypass the same origin restriction on XMLHttpRequests by tricking the proxy into handling a single request as multiple pipe lined requests directed at arbitrary hosts. Source: <http://www.frsirt.com/english/advisories/2005/2147>

29. *October 19, Secunia* — Avaya CMS / IR Solaris Xsun and Xprt privilege escalation vulnerability. A vulnerability has been found in CMS and IR. This can be exploited by malicious, local users to gain escalated privileges. This vulnerability may allow a local unprivileged user the ability to execute arbitrary code with the privileges of either the Xsun(1) or Xprt(1) command. Source: <http://secunia.com/advisories/17246/>

30. *October 19, US-CERT* — Technical Cyber Security Alert TA05-292A: Oracle products contain multiple vulnerabilities. Oracle has released a Critical Patch Update that addresses more than eighty vulnerabilities in different Oracle products and components. The impact of these vulnerabilities varies depending on the product, component, and configuration of the system. Potential consequences include remote execution of arbitrary code or commands, information disclosure, and denial of service. An attacker who compromises an Oracle database may be able to gain access to sensitive information. US-CERT recommends that sites running Oracle review the Critical Patch Update, apply patches, and take other mitigating action as appropriate. Critical Patch Update: http://www.oracle.com/technology/deploy/security/pdf/cpuoct2_005.html Source: <http://www.us-cert.gov/cas/techalerts/TA05-292A.html>

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US-CERT Operations Center Synopsis: US-CERT reports a vulnerability in the Snort Back Orifice Parsing Remote Code Execution the exploit is in Snort's Back Orifice pre-processor. A stack based overflow can be triggered with a single UDP

packet, allowing an attacker to fully compromise a Snort or Sourcefire installation. X-Force believes this vulnerability to be trivially exploitable, and urges affected users to upgrade immediately. Snort is a widely deployed, open source network intrusion detection system (IDS). Snort and its components are used in other IDS products, notably Sourcefire Intrusion Sensors, and Snort is included with a number of operating system distributions.

Snort preprocessors are modular plugins that extend functionality by operating on packets before the detection engine is run. The Back Orifice preprocessor decodes packets to determine if they contain Back Orifice ping messages. The ping detection code does not adequately limit the amount of data that is read from the packet into a fixed length buffer, thus creating the potential for a buffer overflow. The vulnerable code will process any UDP packet that is not destined to or sourced from the default Back Orifice port (31337/udp). An attacker could exploit this vulnerability by sending a specially crafted UDP packet to a host or network monitored by Snort.

US-CERT is tracking this vulnerability as VU#175500 please review:

<http://www.kb.cert.org/vuls/id/175500>

Top Source Port / IP Addresses: Increased reported port activity: 1026 UDP, 1026 UDP, 1029 UDP, 1030 UPD from the following IP blocks, located in China: 221.10.254.31,218. 66.104.208, 222.77.185.242, 221.27.16.180, 61.152.158.126, 221.6.77.72, 202.99.172.160, and 218.66.104.206

US-CERT strongly recommends that all users reference the Federal Emergency Management Agency (FEMA) web site for a list of legitimate charities to donate to their charity of choice. <http://www.fema.gov/>

Current Port Attacks

Top 10 Target Ports	6346 (gnutella-svc), 1026 (win-rpc), 6881 (bittorrent), 445 (microsoft-ds), 26777 (----), 135 (epmap), 139 (netbios-ssn), 40000 (----), 1025 (win-rpc), 25 (smtp) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
----------------------------	--

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

[\[Return to top\]](#)

General Sector

31.

October 20, Associated Press — **Five arrested in Baltimore terror probe.** A fifth man has been arrested during an investigation into a possible terrorism threat to a Baltimore highway tunnel this week, according to court documents. Maged Hussein, who owns an eastern Boston market that was raided by federal authorities on Tuesday, October 18, was taken in to custody on a handgun charge, the documents showed. Four other men were also detained Tuesday on immigration charges and will be deported, according to Mark Bastan, acting special agent in charge at Immigration and Customs Enforcement in Boston. One of those men, 30-year-old Mohamed Ahmed Mohamady Ismail, came up in a tip about the purported tunnel plot from a source who is in custody in the Netherlands, Bastan said.

Source: http://www.usatoday.com/news/nation/2005-10-20-baltimoretunn el_x.htm

[\[Return to top\]](#)

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:

<http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.